

III

0.1 THE PLAN OF THE BOOK

The plan of this history appears in detail in the following Table of Contents: but a few general and preliminary remarks may be useful to the intending reader.

The first section after the Table of Contents is a general introduction, a sketch of the whole history of Hut 6, from the pen of the Head of the Hut, P.S. Milner-Barry. This account should certainly be read before the rest of the book is tackled as it gives a delightfully vivid bird's-eye view of Hut 6 and its life. It is true that it contains some technical terms which may puzzle a reader who comes to the History with no previous knowledge of the subject, but the general lines of the story are clear, and any obscure details are best left to be clarified by a second reading when the reader has delved further into the history.

After this introduction the history proper begins. Most of the main divisions or "Books" correspond to the chief functional divisions of Hut 6 and indeed are such as are almost inevitable in any cryptographic organisation. Traffic must be intercepted, then identified, then registered, then broken and then decoded; each of these operations was performed by a separate section of Hut 6 and to each a separate Book is devoted. The order given above (which is the normal chronological order) has been followed except that for obvious reasons breaking the traffic - the end of the whole process - has been placed first. It now remains to discuss the arrangement of the work within the various Books.

Book 1, CRYPTOGRAPHY, deals with the actual breaking of keys and with the work of the cryptographic sections - i.e. Watch, Research and Machine Room. The treatment throughout is primarily historical: after an introductory description of the machine five chapters follow on the main cryptographic periods of the war. Then two shorter chapters deal with the closely related subjects of Bombe Control and the History of the Machine Room; and finally we have a long chapter on the History of Special Groups of Keys and a short final one of General Comments on cipher security.

Technical details and full descriptions of the processes involved have not been inserted in this history - these will be found in the separately published "History of E/Breaking, Part II". There were three main reasons for taking this course.

(1) Even as matters stand, the Book on Cryptography is the largest division of this work, and if full technical details had been added the Book would have reached too disproportionate a length.

(2) It was believed that there would be considerable gain to clarity of exposition if the technical and historical approaches to cryptography were firmly separated and dealt with in separate works. To deal with them in the same book would have meant that confusing changes of standpoint would have occurred rather frequently.

(3) Technically, the problems of Hut 6 were similar in many respects to those of Hut 8. It was possible to bring this out (as has been done) in a joint Technical History but the problems of Hut 8 could clearly find no place in the history of Hut 6.

The result of the course taken is that the treatment of cryptography in the present work is as little technical as possible (with a few exceptions to be later mentioned). This history is, in short, written for the layman who should consult

the Technical History for further details on any point that has aroused his curiosity. On the other hand, the professional cryptographer may well prefer to read the Technical History first, and consult the present work later for the purpose of filling out the historical background.

The exceptions previously referred to are Chapters 1.0 and 1.1. These do contain a certain amount of technical detail and in fact Chapter 1.0 (which contains the unavoidable minimum of information about the machine) is taken direct from the Technical History. Chapter 1.1 deals with the early history of Hut 6 with which questions of technique are so closely bound up as to make impossible the rigid separation that is later enforced.

The only other comment worth making on Book 1 is that the constantly increasing complexity of the general cryptographic situation is reflected in the increasing length of the historical chapters. The stage was indeed crowded for the Fifth Act.

Book 2, INTERCEPTION, is much simpler in structure. The more technical side will be dealt with in other histories and we have only striven to deal with the matter from the Hut 6 point of view. After a general introduction and a chapter on Stations and Communications, there follows a chapter on the routines and history of the Control Room, the Hut 6 section concerned with interception. This central chapter is followed by a shorter one on the rather special subject of Overseas Interception, a few General Comments and a brief Appendix on Hut 6 Liaison with W.O.Y.G. For statistics of sets the reader is referred to the Statistical Appendix at the end of the whole work. It will be noticed that this Book is arranged by subject, and not, in the first instance, chronologically.

Book 3, TRAFFIC IDENTIFICATION, is apart from Book 1, the longest. Its special peculiarity is that it deals almost wholly with the period from November 1943 onwards when Traffic Identification first became a problem and T.I.S. was set up. Again the Book is arranged primarily by subject after a general introduction. The principle has been to describe in the first instance the normal routine of Initial Sorting and the work of the Duddery, then to discuss the more specialised work of Sector Investigation, first on the Air and then on the Army, with illustrations from specific sectors, and then to deal with the two great Traffic Identification crises in some detail. There is thus a steady progression from the simple to the complex. The final chapter 3.9 is in the nature of an Appendix containing a number of papers on special points, some of which are mainly intended for purposes of reference.

The remaining Books are very much shorter and, for that reason alone, have a clearer outline. In Registration and Decoding an attempt has been made to keep the basic routine quite separate from the refinements introduced to meet special problems and circumstances. The Statistical Appendix and Glossary are naturally mainly designed for reference.

It should perhaps be emphasised that the Books are to a great extent independent and though the order adopted seemed to us the best there is no very cogent reason why the reader should not pick and choose among the Books to suit his taste. But it is certainly advisable to read through in order whichever Book is chosen.

V

0.2 TABLE OF CONTENTS: VOLUME I

0.0	EDITORS PREFACE	I
0.1	PLAN OF THE BOOK	III
0.2	TABLE OF CONTENTS	V
0.3	HUT 6: AN ADVENTURE	1
	0.30 General Retrospect	2
	0.31 1 9 4 0	3
	0.32 1 9 4 1	6
	0.33 1 9 4 2	7
	0.34 1 9 4 3	9
	0.35 1 9 4 4	14
	0.36 1 9 4 5: Finale	20
	0.37 Postscript	22
	0.38 P.S. Milner-Barry	27
	BOOK 1 CRYPTOGRAPHY	29
1.0	THE GERMAN ENIGMA MACHINE	30
	1.01 Preface	30
	1.02 Description	30
	1.03 Method of Use	31
	1.04 Four-Wheel Machine	32
	1.05 Appendix	33
1.1	PERIOD I: PRE-WAR AND SEPTEMBER 1939 - JANUARY 1940: THE BEGINNINGS	34
	1.10 Introductory	35
	1.11 Pre-War: Early Theory	35
	1.110 The First Crib	35
	1.111 Rods and Wheel-breaking	36
	1.112 The Indicating System and Its Vulnerability	39
	1.113 Depth and Turnover	42
	1.114 New Wheels and Indicating System: The Goal-hunt	43
	1.115 News from Poland	44
	1.116 Polish Methods of Key-breaking	45
	1.12 War: The First Successes	47
	1.120 The Outbreak of War	47
	1.121 The Bombe and the Netz	48
	1.122 The Jeffreys Sheets	52
	1.123 Method of Using the Netz	53
	1.124 Early Failures	53
	1.125 Cillies and Attempts at Depth-reading	53
	1.126 The First Breaks of War-time Keys	55

1.2 PERIOD II: JANUARY TO JULY 1940: SITTENBIEG, NORWAY, FRANCE: START OF CONTINUOUS OPERATIONAL BREAKING 56

1.20 From January to March 57

1.201 Red, Blue and Green 57

1.202 Success and Early Organisation 57

1.21 Operational Breaking 58

1.210 Rise of Yellow 58

1.211 The New Indicating System: First Great Crisis of Hut 6 59

1.212 Overwhelming Importance of Red 60

1.213 Hand Breaks 60

1.22 The Rules of Keys 63

1.220 General Considerations 63

1.221 The Rules of Red 64

1.222 Results of the Discoveries 64

1.223 Rules of Other Keys 65

1.224 Red Keys, June 1940 65

1.23 Daily Procedure in Machine Room 68

1.24 Liaison with France 69

1.3 PERIOD III: AUGUST 1940 - MAY 1941: BRITAIN ALONE: RISE OF BOMBS AND THE CRIB ROOM 70

1.30 General Historical Summary 71

1.31 Arrival of the Bombe: What it Did 72

1.32 The Establishment of the Crib Room 74

1.33 New Discoveries in Rules of Keys: Brown 75

1.34 The Origins of Research 77

1.340 The Function of Research 77

1.341 Early Organisation and Methods 77

1.342 Early Triumphs 77

1.343 Summary 79

1.4 PERIOD IV: JUNE 1941 - DECEMBER 1943: WORLD WAR: THE GREAT PERIOD OF EXTENSION AND CONSOLIDATION 80

1.40 General Historical Summary 81

1.400 Features of the Period 81

1.401 Increase of Keys 81

1.402 Increase of Personnel 82

1.403 Increase of Machines 82

1.404 Growing Complexity of Organisation 82

1.405 Technical Developments 83

1.406 General Course of Breaking 83

1.407 Liaison with Sixta 84

1.408 Liaison with Hut 3 84

1.409 Conclusion 85

1.41	Detailed Theory of Rules of Keys	87
1.410	Sources of Information	87
1.411	Air and Army	87
1.412	Divisions of the Subject	87
1.413	Wheelorder Rules: Army and Air	87
1.414	Setting up of Committee on Rules of Keys	91
1.415	Ringstellung Rules: Army and Air	92
1.416	Stecker Rules: Air and Army	94
1.417	Brown Rules	96
1.42	G.A.F. Key Repeats	99
1.420	Institution of Key Records	99
1.421	Limitation of the Subject	99
1.422	Local Keys	99
1.423	Keys Constructed by the Cipher Office: Repeats in 1941	99
1.424	1942: Quadrilateral Repeats	100
1.425	Effects on Our Breaking Policy	101
1.426	Effects on Our Intercept Policy	101
1.427	Repeats in 1943 and 1944	102
1.428	Stecker/D Repeats in 1945	102
1.429	Conclusion	104
1.43	General Organisation of Machine and Crib Rooms later Watch and Research	105
1.430	The Fourfold Division	105
1.431	Location of Rooms	105
1.432	Subordination of Sub-sections	105
1.433	The Differentiation of Function	106
1.434	Dissatisfaction in the Machine Room	106
1.435	The Problem Solved	107
1.436	The Formation of Research	107
1.437	The Parentage System	108
1.438	Some Special Points	110
1.439	Summary	110
1.44	Training Schemes in Hut 6	112
1.440	Early Training	112
1.441	The Beginnings of the Schools	112
1.442	The R.R. School Syllabus	113
1.443	Watch and Research Training	114
1.444	The Outline Course and Special Talks	115
1.445	Other Educational Systems	116
1.5	PERIOD V: JANUARY 1944 - MAY 1945: THE LIBERATION OF EUROPE: HUT 6 FIGHTS BACK AGAINST NEW GERMAN SECURITY DEVICES	118
1.50	General Historical Summary	119
1.500	The Determining Factors	119
1.501	The Technique of Cryptography	119
1.502	The Organisation of Cryptography	119
1.503	Importance of Other Sections to Cryptography	119
1.504	Contribution of Hut 6 to Intelligence	120

1.51	German Security Devices and Our Counter-	121
	Measures: Reflector D	
1.510	General Introduction	121
1.511	Reflector D in General	121
1.512	January to July 1944	122
	The First Menace	122
	Illusory Triumph	123
	The <u>BO</u> Mystery	123
	The D Substitution	124
	Greenshank and D	125
	Red D's: January to July	126
	The Overhanging Menace	126
	Preparations for August 1	127
1.513	August 1944 - May 1945	127
	Extension of D	127
	Effects on Breaking	129
	D-Breaks	130
	D-Captures	131
	D Rules	131
1.514	Summary of the German Use of D	132
1.515	Appendices	133
	D Statistics, Key by Key	133
	Chronological List of D's broken	
	without a Prior Break on	
	Reflector B	134
	Graph of Progress in Recovering D's	135
1.52	German Security Devices: Enigma Uhr	136
1.520	The Problem	136
1.521	Routine Adopted	136
1.522	Extension of Enigma Uhr	136
1.523	Effect on Breaking	137
1.524	Uhr Notation	137
1.525	Summary	138
1.526	Appendix: Uhr Statistics	138
1.53	German Security Devices: Zusatz Stecker	139
1.530	The May Scare	139
1.531	A Damp Squib	139
1.532	Extent of Change	140
1.533	The German Idea	140
1.54	German Security Devices: Notschlüssel	141
1.540	Introduction	141
1.541	First System	141
1.542	First Appearance of the NOTS	141
1.543	The Saga of Guernsey or the	142
	Qwatch and the Forty NOTS	
1.544	The Plague of NOTS	142
1.545	NOT-keys, New Style	146
1.546	Conclusions	147
		150

1.55	Other German Security Devices	152
1.550	CY	152
1.551	Random Indicators	154
1.552	Wahlworts	156
1.553	The Mosse Code	160
1.554	Double Encoding	161
1.56	The Change from Watch/Research to Air/Army	163
1.560	Introductory	163
1.561	Stages of the Change	163
1.562	Reasons for the Change	163
1.563	Results of the Change	164
1.564	Timing of the Change	165
1.565	Unity of Control	166
1.57	The Organisation of the Watch	167
1.570	Introduction	167
1.571	The Function of the Watch	167
1.572	Basic Organisation	167
1.573	Division of Keys between Watches	168
1.574	Watch A (three shifts)	168
1.575	Watch Q	169
1.576	Watch M (three shifts) and Watch R (one shift)	170
1.577	BCVO (two shifts)	170
1.578	Administration	171
1.579	Appendix: Detailed Distribution of Members	172
1.58	Final Developments of the Rules of Keys	173
1.580	Introduction	173
1.581	The Regular Air Keys	173
1.582	Brown, Yak and Llama	174
1.583	Army Keys	175
1.584	Rules of D's	176
1.585	Summary	177
1.6	BOMBE CONTROL	178
1.60	Introduction	179
1.61	The Problem	179
1.62	"Intelligence Value"	179
1.63	Hut 6 - Hut 8	180
1.64	Hut 6 Keys	181
1.641	Responsibility	181
1.642	Daily Meeting	181
1.643	Priority List	181
1.65	Current Bombe Control	182
1.651	England	182
1.652	Washington (Op-20-G)	183
1.653	Washington (Arlington)	184
1.66	Conclusion	184

1.7	HISTORY OF THE MACHINE ROOM (FORMERLY NETZ ROOM)	185
1.70	Historical Outline	186
1.71	Expansion of the Room	186
1.72	The Breaking of Duds	187
1.73	Final Set-up for Bombe Control	188
	1.730 Communications	188
	1.731 Routine Organisational Jobs	188
	1.732 Normal Testing of Stops	190
	1.733 Special Problems	190
1.8	HISTORIES OF SPECIAL GROUPS OF KEYS	192
1.800	General Introduction	193
1.801	Red	194
	1.8010 Red: A Major German Blunder	194
	1.8011 Breaking, 1940 - 1945	194
	1.8012 Supreme Importance of Red	195
	1.8013 Blue and Pink	196
1.802	Brown	198
	1.8020 Introduction	198
	1.8021 "Target for Tonight"	199
	Phase I: September 1940 - May 1941	
	Phase II: December 1941 - June 1942: Brown II	201
	1.8022 The Lull: Brown I	201
	1.8023 Attack and Defence	204
	Brown IV	204
	Brown III	204
	1.8024 Conclusion	206
	1.8025 Appendix: Example of Depth on Brown I	208
1.803	The Mediterranean Air Keys	209
	1.8030 General	209
	1.8031 The Triangle	210
	1.8032 The African Campaign	210
	1.8033 The Italian Campaign	212
	1.8034 The Balkans	213
	1.8035 The Last Months	215
1.804	The African Army Keys	217
	1.8040 General	217
	1.8041 The First Breaks: 1941 - 2	217
	1.8042 The Re-entry into Chaffinch, April 1942	218
	1.8043 April - October: Improvement in Technique and Increasing Success	219
	1.8044 Phoenix: the Difficulties of Overseas Interception	220
	1.8045 The Wahlwort Era: The Phoenix- Finch Complex: December 1942 - April 1943	221

1.8046	Thrush (Sonder M/S Rom- Malemes and Other Keys	223 225
1.8047	Appendix	226
1.805	The Italian Army Keys	226
1.8050	General	226
1.8051	Before the Surrender of Italy, May - September 1943	226
1.8052	Surrender of Italy and Rise of Shrike and Bullfinch: September 1943 - February 1944	227 228
1.8053	Kingfisher: May - August 1944	228
1.8054	Revival of Albatross: October 1944 - May 1945	228 229
1.8055	The Puffins	229
1.8056	Sparrow	231
1.806	The Balkan Army Keys	231
1.8060	General	231
1.8061	Before the Italian Surrender: February 1942 - September 1943	231
1.8062	Surrender of Italy: Appearance of Wryneck: September 1943 - November 1944	233
1.8063	Arrival of Russians and New Balkan Set-up, November 1944	235
1.807	The Western Air Keys	236
1.8070	General	236
1.8071	The Breaking of Snowdrop	236
1.8072	The Pivotal Importance of Red	237
1.8073	The Further Growth of the Re- encodement Complex	237
1.8074	D Day	238
1.8075	The Period of Regular Breaking	238
1.8076	Changes in Emphasis	240
1.8077	The Decline of the West	240
1.808	The Western Army Keys	243
1.8080	General	243
1.8081	Before D Day	243
1.8082	D Day and the First Breaks	245
1.8083	The First Lull	245
1.8084	The Breakthrough	246
1.8085	The Second Lull: October	246
1.8086	The Final Battles: Heavy Traffic Once Again	249
1.809	The German Air Keys	251
1.8090	General	251
1.8091	Research	251
1.8092	The Watch	251
1.8093	The First Phase	252
1.8094	The Second Phase	253
1.8095	The Third Phase	253 254

1-810	The Eastern Air Keys	256
1-8100	General	256
1-8101	The German Advance	258
1-8102	Key Repeats	258
1-8103	Hedgehog	259
1-8104	The Heyday of Research	259
1-8105	The Problem of the Luftflotten	261
1-8106	The End	262
1-811	The Eastern Army Keys	264
1-8110	General	264
1-8111	Initial Advances, June - December 1941	264
1-8112	Quiescence, 1942 - 3	264
1-8113	Spread of Use of Local Keys, July 1943 - December 1944	265
1-8114	The Final Spurt	266
1-812	Greenshank and Allied Keys	267
1-8120	The Main Features of Greenshank	267
1-8121	Breaks, 1939 - 1942	268
1-8122	A Blank Wall	269
1-8123	Inside Information	269
1-8124	The Mystery Solved	270
1-8125	The Last Phase: Statistics and Summary	271
1-8126	The Associated Keys: Falcon, Gannet II, Mallard	272
1-8127	The Breaking of Nuthatch	273
1-8128	Grouse and the Wehrkreis CQ Key	274
1-8129	The Rôle of W.O.Y.G.	274

I

TABLE OF CONTENTS : VOLUME II

TABLE OF CONTENTS I

1·8 HISTORIES OF SPECIAL GROUPS OF KEYS (continued)	1
1·813 S.S. and Police Keys	1
1·8130 General Characteristics	1
1·8131 History to the End of 1941	2
1·8132 1942: The Orange Age	5
1·8133 1943-5: The Quince Age	12
1·8134 Summary	13
1·814 Mustard	13
1·8140 Introduction	13
1·8141 Russian Mustard: Mustard I, IV	13
1·8142 Mediterranean Mustard: Mustard II, III	14
1·8143 Western Mustard and Cress	16
1·8144 The End of the Story	16
1·815 The V-Keys	17
1·8150 General Introduction	17
1·8151 Corncrake	17
1·8152 Ibis	19
1·8153 Jerboa	23
1·8154 Importance of the V-Keys	23
1·816 First Breaks of Keys	26
1·9 SUMMARY AND CONCLUSIONS	32
1·90 General	33
1·91 How Breaks are Secured	33
1·92 How Breaks can be Prevented	34
1·920 The Three Desiderata	34
1·921 The Two Roads	34
1·922 The Principle of Over-protection	35
1·93 The German Enigma	35
1·930 Theoretical and Practical Security	35
1·931 The Failure of German Efforts	35
1·932 Air and Army Security	35
1·933 The Special Case of Greenshank	36
1·94 How to Achieve Security	36
1·95 The Necessity of Supervision	37
BOOK 2 INTERCEPTION	39
2·0 GENERAL INTRODUCTION	40
2·00 The Beginnings	41
2·01 The Growth of Control: Early Problems	41
2·02 Plan of This Book	42

2.1	INTERCEPT STATIONS AND COMMUNICATIONS	43
2.10	Introduction	44
2.11	History of Station Development	44
2.110	Home Stations: Increase of Sets	44
2.111	Home Stations: Communications	46
2.112	Overseas Stations: General History	47
2.113	Overseas Stations: Increase of Sets	47
2.114	Overseas Stations: Communications	49
2.12	Description of Intercept Stations	50
2.120	Beaumanor and Bishop's Waltham	50
2.121	Chicksands	50
2.122	Forest Moor	51
2.123	The Smaller Stations	51
2.2	CONTROL (HOME INTERCEPTION)	52
2.20	Introduction	53
2.21	General Function and Theory	53
2.210	General Outline	53
2.211	Task Allocation and Priorities	53
2.212	Control as Liaison Agent with the Stations	54
2.22	Methods and Records	55
2.220	Introduction	55
2.221	Incoming Information	55
2.222	Control Records	55
2.223	Routine Duties in the Control Room	56
2.224	Services Rendered	57
2.225	Communications	58
2.226	Conclusion	58
2.23	Staff	60
2.24	Historical Account	60
2.240	The Early Days	60
2.241	1942: A Year of Development	62
2.242	1943: A Year of Specialisation and German Security Measures	63
2.243	1944: New Callsign Systems and Invasion Commitments	64
2.244	1945: Callsign Encoding	66
2.245	Retrospect	66
2.3	OVERSEAS INTERCEPTION	67
2.30	Function and Peculiar Differences	68
2.31	Description and Role of the Overseas Party	68

2.4 PARTICULAR COMMENTS	70
2.41 Initial Mistakes	71
2.42 Sixta Controversy	72
2.420 Introduction	72
2.421 Statement of the Case	72
2.422 Reflection	72
2.43 Liaison with Intercept Stations	73
2.430 The Need for Contact	73
2.431 Resident Liaison Officers at Intercept Stations	73
2.432 Interchange of Visits	73
2.433 The Problem Reviewed	74
2.5 HUT 6 LIAISON AT W.O.Y.G.	75
2.50 Introduction	76
2.51 Duties of the Hut 6 Party	76
2.52 Keeping the Cover List	76
2.53 Watching New Groups	77
2.54 Direct Help to Cryptographers	77
2.55 Assisting the C.R.R.	78
2.56 Long-term Research	78
2.560 Classification of Problems	78
2.561 Immediate Developments	79
2.562 Problems Requiring Collection of Data	79
2.563 Recurring Problems	79
2.564 Cryptographic Problems	80
2.565 Failures	80
2.57 General Intercept Policy	80
2.58 Conclusion	80
BOOK 3 TRAFFIC IDENTIFICATION	81
3.0 GENERAL HISTORICAL REVIEW	82
3.00 Introduction : 1939 - November 1943	83
3.01 The Birth of T.I.S.	84
3.010 The November 1943 Crisis	84
3.011 The Problem	85
3.012 The Measures Taken	85
3.02 1944 to the End	88
3.020 The April 1944 Crisis	88
3.021 Changes in Organisation	88
3.022 Initial Sorting	89
3.023 Sector Investigation	92

3-024	Establishment of T.I.S.1 and T.I.S.2	92
3-025	From Watch/Research to Air/Army	92
3-026	The Heyday of T.I.S.	93
3-027	T.I.S.2 from D Day	94
3-028	February 1945: The Crisis	96
3-029	February 1945: The Aftermath	99
3-1	INITIAL SORTING	101
3-10	Introduction	102
3-11	1939 - September 1943	102
3-12	September 1943 - April 1944	103
3-13	April 1944 - February 1945	105
3-14	Conclusion	109
3-15	Diagrams:	110
	Initial Sorting System, January, 1944	110
	Initial Sorting by Serial, August, 1944	111
3-2	THE DUDDERY	112
3-20	Introduction	113
3-21	Persomel	113
3-22	The System of Processing Duds	114
3-23	The Technique of Dedudding	115
3-230	Definition	115
3-231	Indicator Corrections	115
3-232	T.O.O. and T.O.I. Corrections	115
3-233	Wrong Periods	115
3-234	Back Days' Keys	115
3-235	Special Codes and Enigma Uhr	116
3-236	Special Information	116
3-24	Liaison with T.I.S.1	116
3-3	T.I.S.1: G.A.F. SECTOR AND DISCRIMINANT INVESTIGATION	117
3-30	Introduction	118
3-31	The Sectors and their Keys	119
3-32	Sources of Information	122
3-320	General Classifications	122
3-321	Traffic	123
3-322	Source Evidence	127
3-323	Log Evidence	129

3.33	Air Discriminant Investigation	131
3.330	General	131
3.331	The Development of the Discriminant Identification System	131
3.332	Methods of Identification	132
3.333	Duties of Discriminant Investigators	133
3.334	General Observations on the G.A.F. Use of Discriminants	133
3.335	Statistics	134
3.4	T.I.S.2 AND ARMY TRAFFIC IDENTIFICATION	135
3.40	Introduction	136
3.41	November 1943 - April 1944	136
3.410	General Features	136
3.411	Organisation of the Quiet Room	136
3.412	Blisting of Army Traffic	140
3.413	The Special Case of Western Front Army Traffic	140
3.42	May - October 1944	141
3.420	Reorganisation of T.I.S.	141
3.421	The Army Sector System	141
3.43	November 1944 - May 1945	143
3.430	The Heyday of T.I.S.2	143
3.431	The Loss of Serialising Callsigns	143
3.432	The Army Notation System	143
3.433	The Backwash of the February Air Crisis	145
3.5	THE MAIN NETWORKS OF THE GERMAN ARMY	147
3.50	Introduction: Sector Investigation in T.I.S.2	148
3.51	The Western Front : D Day to Autumn 1944	150
3.510	The Problem after D Day	150
3.511	The German Radio Network	150
3.512	Sorting to Blists	151
3.513	The Sector Investigator and Registration	151
3.514	The Sector Investigator and Decoding	152
3.515	Analysis of Discriminants	153
3.516	Identification of Broken Keys	153
3.517	Captured Keys and Equipment	153
3.518	Staff and Organisation	154
3.52	The G.H.Q. Sector	155
3.520	Origin of the Sector	155
3.521	The W/T Problem of the G.H.Q.	155
3.522	The Keys Used	156
3.523	Discriminant Sorting	157
3.524	Action on Breaks	157

3.6	THE GREATER GERMANY SECTOR	159
3.60	Greater Germany Keys	160
3.61	The Wehrkreis System	160
3.610	W/T Set-up	160
3.611	Keys	161
3.612	Breaks	162
3.613	Sector Investigator's Duties	162
3.62	The Falcons	163
3.620	Falcon Redivivus	163
3.621	The Sorting Problem of Falcon	163
3.622	W/T Set-up	164
3.623	The Twofold Investigation Problem	164
3.624	Analysis of Broken Traffic: Outs	165
3.625	Analysis of Broken Traffic: Duds	165
3.626	Discriminating Falcon	165
3.7	APRIL 1, 1944	167
3.70	The Problem	168
3.71	Liaison	169
3.710	General	169
3.711	Control and Interception	169
3.712	Direction Finding and Radio Finger Printing	169
3.713	Sixta	170
3.714	Air Section	170
3.72	Operations	171
3.720	The Function of the General Staff	171
3.721	Band Sorting and Callsign Conversion	172
3.722	The Function of the Giant Foss	173
3.723	The Function of I.C.X.	174
3.724	Function of the Identification Party	175
3.725	The Back-Room Organisation	175
3.73	Conclusion	177
3.8	FEBRUARY 1, 1945	179
3.80	The General Nature of the Crisis	180
3.81	The Crisis in Detail	181
3.810	Definition of Terms	181
3.811	The G.A.F. Discriminant Book	181
3.812	Help from Intercept Operators	182
3.813	Evidence of Low-grade Ciphers	182
3.814	The Role of Sixta	183

3*82	Preparations for the Crisis	183
3*820	The German Forewarning	183
3*821	Preparation of the Plan	183
3*822	Divisions in the Sorting Process	184
3*823	The New Air Notation System	184
3*83	Current R.R. Air Sorting	184
3*830	The ^{ANS} Menus: Records	184
3*831	The ^{ANS} Menus: Source of Information	186
3*832	Personnel	186
3*833	The Plan in Action	187
3*834	Practical Snags: Duds, Clashes and Tries	188
3*84	Back-Room Sorting	189
3*840	Redistribution of Staff	189
3*841	Unidentified Traffic Analysis	190
3*842	Key-break Analysts	190
3*843	Bleaners	190
3*844	Discriminant Analysis	191
3*85	Further Developments of the Crisis	191
3*9	MISCELLANEOUS TOPICS : TRAFFIC, DISCRIMINANTS AND KEYS	193
3*90	Traffic Characteristics	194
3*900	Army/Air Differences in General	194
3*901	Time of Origin	194
3*902	Priority Symbols	194
3*903	Discriminants	195
3*904	Length of Messages	195
3*905	Miscellaneous	195
3*91	German Air Force Discriminants	196
3*910	Introduction	196
3*911	The First Book	196
3*9110	Period of Validity	196
3*9111	Format and Contents	197
3*9112	First Phase: December 1939 to February 1943	197
3*9113	Second Phase: March 1943 to August 1943	200
3*912	The Second Book	204
3*9120	Period of Validity	204
3*9121	Format and Contents	204
3*9122	Cipher Office Procedure	204
3*9123	Recording of Discriminants	204
3*9124	Reconstruction	204

3*913	The Third Book	205
3*9130	Its Introduction	205
3*9131	Format and Contents	205
3*9132	Procedure of the Cipher Office	206
3*9133	Recording of Discriminants	209
3*9134	Reconstruction	209
3*9135	Defects of the German System	212
3*9136	How it Could have been Done	214
3*914	Key Numbers	214
3*915	List of Appendixes	214
	Appendix 1	215
	Appendix 2	216
	Appendix 3	217
3*916	Postscript	218
3*92	German Army Discriminants	220
3*920	General	220
3*921	The Three Books	220
3*922	Book I	220
3*923	Book II	221
3*924	Book III	221
3*925	<i>Some Examples of Discriminant Usage</i>	223
3*93	English Key Names of Air and Army Keys	225
3*930	The Early Days	225
3*931	Air Keys	225
3*932	Army Keys	227
3*94	General Use and Distribution of G.A.F. Keys	229
	Appendices	235
	Table A: List by German Categories of G.A.F. Keys	235
	Table B: Alphabetical List under English Name of all G.A.F. Keys	237
	Table C: List of County Keys	245
3*95	General Use and Distribution of Army Keys	247
	Appendices	250
	Table A: The Various Categories of German Army Keys Operative in March 1945	250
	Table B: List of all German Army Keys Identified During the War	253
	Table C: Key Set-up in Area of Heeresgruppe G (Western Front) in November 1944	262

1

TABLE OF CONTENTS: VOLUME III

Book 4: TRAFFIC REGISTRATION	1
4.0 THE NORMAL FUNCTIONS OF THE REGISTRATION ROOM	2
4.00 General Outline of History	3
4.01 Technical Processes	3
4.010 General	3
4.011 Blisting	4
4.012 Fossing	5
4.013 Treatment of Horrors	5
4.014 Kissing	5
4.015 Ticking-off	6
4.016 Sorting	6
4.017 Operation of the Hanky-Panky Diagrams	7 8
4.1 SPECIAL REGISTRATION PROBLEMS	9
4.10 Western Front Army Traffic	10
4.100 History	10
4.101 Sorting Procedure	10
4.102 Broken Keys	10
4.103 Special Duties of the W/F Party	10
4.104 Composite Blisting in General	11
4.105 The W/F Composite Blist	11
4.106 The Composite Tick-off System	11
4.107 Disposition of Duds	12
4.11 The Work of R.R. 2 (Later R.R. Army)	12
4.110 Blisting Procedure	12
4.111 Miscellaneous Functions of R.R. 2	13
4.112 The Change to R.R. Army	13
4.2 GENERAL ORGANISATION	15
4.20 The R.R. Libraries	16
4.21 R.R. Staff and Administration	16
Book 5: TRAFFIC DECODING	18
5.0 HISTORY AND ORGANISATION OF THE DECODING ROOM	19
5.00 General Historical Summary	20
5.01 Basic Organisation	21
5.010 Personnel and Shifts	21
5.011 Technical Duties of the D.R. Head	21
5.012 Administrative Duties of the D.R. Head	22
5.013 Duties of Heads of Shifts	22
5.014 Training of New Members	23

5.1	THE NORMAL ROUTINE OF THE D.R.	24
5.10	Description of Machines	25
5.11	Care and Maintenance	25
5.12	Routine of Breaks	26
5.120	Setting up the Machines	26
5.121	Keeping of Records	27
5.122	Routeing of Traffic into D.R.	27
5.123	The Tick-off	27
5.124	Routeing of Decodes and Duds from D.R.	28
5.125	The Tally Sheets	28
5.13	Decoding Priorities	29
5.14	The Technique of Decoding	29
5.140	General Rules	29
5.141	Dealing with Corrupt Texts	30
5.142	Faulty Turnover	30
5.143	Nuthatch and Greenshank	31
5.144	Menus and Grass Skirts	31
5.145	"D.R.'s"	31
5.146	Duds	32
5.147	Oddments	33
5.148	Dupes	33
5.2	GERMAN SECURITY DEVICES AND THEIR EFFECTS ON THE D.R.	34
5.20	General Introduction	35
5.21	Wheelorders	35
5.22	R, S, T	35
5.23	F Messages	36
5.24	Reflector D	36
5.25	Enigma Uhr	37
5.26	Miscellaneous Snags	38
5.27	The Last Straw: Encoded Callsigns	39
Book 6:	ORGANISATION AND ADMINISTRATION	41
6.0	FUNCTIONS OF THE GOVERNING BODY	42
6.00	1941: Institution of the Governing Body.	43
6.01	1942: Regular Routine of the Governing Body	43
6.02	1943: Expansion of the Governing Body	43
6.03	1945: Dissolution of the Governing Body	44
6.1	ADMINISTRATION OF HUT 6	45
6.10	Duties of the Hut 6 Office	46

6.11 The Work of the Duty Officer	47
6.110 Brief History	47
6.111 General Functions	47
6.112 Summary	47
Book 7: GENERAL COMMENTS	48
7.0 THE EXPERIENCE OF HUT 6 AND ITS RELEVANCE TO THE FUTURE	49
7.00 Introduction	50
7.01 Essential Elements of the Hut 6 Problem	50
7.1 THE MISTAKES OF HUT 6	52
7.10 Introduction	53
7.11 Liaison with Sixta	53
7.12 Liaison with Hut 3	54
7.2 SOME GENERAL POINTS OF CRYPTOGRAPHIC ORGANISATION	55
7.20 Introduction	56
7.21 Specialisation or All-round Knowledge	56
7.22 The Preservation of General Interest	56
STATISTICAL APPENDIX: TABLES AND GRAPHS	58
Comparative Chronological Table	60
Plan of Hut 6, April 1945	68
Traffic Lanes, Hut 6: Summer 1944	69
Internal Relations, Hut 6: Summer 1944	70
External Relations, Hut 6: Summer 1944	71
Traffic, Breaks and Decodes: Statistical Table	72
Graph: Total Traffic Intercepted, 1941 - 5	73
Graph: Total Number of Sets, May 1942 - 5	74
Graph: Teile per Set per Day, 1943 - 5	75
Graph: Fractures: Weekly Totals for G.A.F., Army, S.S. and Railways, 1944 - 5	76
Graph: Fractures: Monthly Combined Totals	77
Graph: Decodes: Weekly Totals, May 1944 - 5	78
Bombe Statistics: Introductory Note	79
Specimen of Daily Time Sheet Issued by Bombe Outstation	80

Specimen of Daily Record Sheet Giving Monthly Totals	81
Analysis of Machine Performances	82
Standard Machines: I General Statistics	82
II Average Times	84
III Analysis of Delays	86
Special Machines: I General Statistics	87
II Average Times	90
III Analysis of Delays	92
GLOSSARY	94